Deutscher Bundestag **Drucksache 19/9605**

19. Wahlperiode 23.04.2019

Antwort
der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Joana Cotar, Uwe Schulz, Dr. Michael Espendiller, weiterer Abgeordneter und der Fraktion der AfD – Drucksache 19/9112 –

Starke Ende-zu-Ende-Verschlüsselung – ohne Nachschlüssel

Vorbemerkung der Fragesteller

Verschlüsselungstechnologien leisten nach Ansicht der Fragesteller einen grundlegenden Beitrag zur IT-Sicherheit. Während die Digitalisierung immer tiefer und breiter in persönliche sowie gesellschaftliche Bereiche Einzug hält, wird immer deutlicher, dass IT-Sicherheit oberste Priorität haben muss, sowohl bei den Markttteilnehmern als auch für die Legislative. Neben Webdiensten und E-Mail-Kommunikation ist davon auszugehen, dass die weltweite Anzahl von Internet-of-Things-Geräten (IoT) von schätzungsweise 21 Milliarden im Jahre 2018 auf über 50 Milliarden Geräte im Jahre 2022 ansteigen wird (www.juniperresearch.com/press/press-releases/iot-connections-to-grow-140-to-hit-50-billion). Alleine Siemens beschäftigt 1 275 Mitarbeiter im Bereich der IT-Sicherheit und ist zirka 1 000 Angriffen pro Tag ausgesetzt. Bitkom e. V. sieht Deutschland aufgrund seiner weltmarkführenden Industrie im besonderen Fokus krimineller Akteure (www.faz.net/aktuell/wirtschaft/diginomics/43-milliarden-euro-schaden-durch-hackerangriffe-15786660.html). Darüber hinaus ist die deutsche Wirtschaft durch das Ausspionieren ausländischer Geheimdienste gefährdet (www.welt.de/wirtschaft/article162217929/So-spionieren-Geheimdienste-deutsche-Firmen-aus.html). Die Bedeutung guter Verschlüsselungsstandards ist für Deutschland besonders relevant, da sich der weltweit größte Internet-Knotenpunkt, DeCiX, in Frankfurt am Main befindet. Daher hat der britische Geheimdienst General Communications Headquarters (GCHQ) kürzlich über seinen Ausleger National Cyber Security Center (NCSC) seinen Einfluss auf das Europä-ische Institut für Telekommunikationsnormen (ETSI) wahrgenommen und versucht (www.sueddeutsche.de/digital/tls-verschluesselung-1.4317326), statt des abhörsicheren Verschlüsselungsstandards TLS 1.3 das mit Nachschlüssel versehene Protokoll „Enterprise Transport Security“ (ETS, vormals eTLS „Enterprise TLS“) zumindest für interne Netzwerkkommunikation zu etablieren. Datenschutzexperten warnen strengstens davor, eine Verschlüsselungstechnologie einzusetzen, welche Nachschlüssel oder ähnliche Abhörmaßnahmen ermöglicht, unabhängig davon, ob Kommunikationsdaten über das Internet oder interne Netzwerke transportiert werden sollen (www.security-insider.de/etls-hebelt-forward-secrecy-von-tls-13-wieder-aus-a-782663/). Ein wichtiger Schritt zu mehr IT-Sicherheit ist die Überarbeitung des Produktsicherheitsrechts (https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fn

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 17. April 2019 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

jw%2F2019%2Fcont%2Fnjw.2019.625.1.htm&pos=5). Dies hat die Bundesregierung richtiger Weise erkannt und auch im Koalitionsvertrag zwischen CDU, CSU und SPD festgeschrieben (Zeilen 6371 – 4375: „Wir werden das Produktsicherheitsrecht novellieren, um die IT-Sicherheit in verbrauchernahen Produkten zu erhöhen. Dazu werden wir u. a. das Produkthaftungsrecht anpassen, Mindeststandards vorschreiben und die Einführung einer gewährleistungsähnlichen Herstellerhaftung prüfen. Darüber hinaus werden wir ein europaweit gültiges IT-Sicherheits-Gütesiegel etablieren.“), allerdings wurde von dem Vorhaben noch nichts umgesetzt. Auch die Verbraucherschutzzentralen äußern Unzufriedenheit bezüglich der bisher nicht erfolgten Einführung einer gewährleistungsähnlichen Herstellerhaftung sowie der Überarbeitung der europäischen Produkthaftungsrichtlinie (www.vzbv.de/content-wrapper/produkthaftung-der-digitalen-welt-staerken). Erste Erfahrungswerte hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) durch die Migration von TLS 1.0 auf TLS 1.2 in den Bundesbehörden sammeln können (www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/BSI_veroeffentlicht_Mindeststandard_fuer_verschluesselte_Internetverbindungen_08102013.html), die bei der Migration auf den nächsten Standard dienlich sein sollten. Ob Nachschlüssel bzw. Hintertüren in internen Netzwerken als sinnvoll erachtet werden, scheint innerhalb des BSI noch strittig zu sein (www.sueddeutsche.de/digital/tls-verschluesselung-1.4317326). Die Landesbeauftragte für Datenschutz in Schleswig-Holstein, Marit Hansen, warnt: „Jeder, der versucht, da [gemeint ist der TLS-1.3-PFS-Standard] nun wieder Hintertüren einzubauen oder Schwächen für diese Sicherheit, der hat gerade nicht verstanden, dass es uns um eine starke Absicherung geht, der sabotiert die Infrastruktur, auf die wir unsere Informationsgesellschaft aufgebaut haben und ich halte diejenigen auch für Hasardeure“ (www.sueddeutsche.de/digital/tls-verschluesselung-1.4317326). Auch Mark Zuckerberg hat die Relevanz von durchgehender Kommunikationssicherheit erkannt und wird bei Facebook Ende-zu-Ende-Verschlüsselung vorantreiben (www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/). In Deutschland ist die IT-Sicherheit mit 9 Prozent Wachstum ein wesentlicher Treiber der IT-Branche (www.bitkom.org/Presse/Presseinformation/Markt-fuer-IT-Sicherheit-erstmals-ueber-4-Milliarden-Euro.html). Höchste Datensicherheit, vor allem bei der Internetkommunikation, steht also nicht im Widerspruch zu Innovationsfähigkeit und Wirtschaftswachstum.

1. Teilt die Bundesregierung die Einschätzung der europäischen ETSI, dass durch die geplante Migration zur Transportverschlüsselung gemäß TLS 1.3 „Chaos“ und „enormer Schaden“ entstehen kann (www.heise.de/newsticker/meldung/Europaeische-Standards-Organisation-warnt-USA-vor-TLS-1-3-4324155.html)?

Die Bundesregierung begrüßt die Einführung von TLS 1.3 und sieht eine Umsetzung in der Bundesverwaltung als sinnvoll an. TLS 1.3 stellt aus kryptographischer Sicht eine Verbesserung gegenüber niedrigeren TLS-Versionen dar. Die Nutzung dieser Protokollversion (mit geeigneten Cipher-Suiten) ist daher zu empfehlen (vgl. Antwort zu Frage 8).

2. Teilt die Bundesregierung die Ansicht der Fragesteller, dass Nachschlüssel jeglicher Art ein Sicherheitsrisiko, sowohl für Endanwender als auch IT-Betreiber, darstellen?

Die Bundesregierung hat ihre grundsätzliche Haltung zum Thema Verschlüsselung in den Eckpunkten der deutschen Kryptopolitik (Kabinettbeschluss vom 2. Juni 1999) festgelegt. Danach hält die Bundesregierung an den als „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ bekannten Säulen der deutschen Kryptopolitik fest. Sie entsprechen der Cybersicherheitsstrategie

der Bundesregierung 2016 und den Vorhaben des Koalitionsvertrags, neben der Stärkung und Förderung der Ende-zu Ende-Verschlüsselung zugleich sicher zu stellen, dass die Sicherheitsbehörden ihre bestehenden Befugnisse auch in der digitalen Welt anwenden und durchsetzen können. Der Einsatz von Nachschlüsseln schwächt die Cybersicherheit und steht damit im Widerspruch zur deutschen Kryptopolitik.

3. Welche Empfehlungen hat die Bundesregierung gegenüber ETSI hinsichtlich der Entwicklung des eTLS ausgesprochen, sei es direkt oder durch beauftragte Experten (www.heise.de/newsticker/meldung/Europaeische-Standards-Organisation-warnt-USA-vor-TLS-1-3-4324155.html)?

Die Bundesnetzagentur hat im Auftrag der Bundesregierung bei ETSI hinsichtlich der Entwicklung des eTLS keine Empfehlungen ausgesprochen.

4. Hat die Bundesregierung Kenntnisse über die Empfehlungen von weiteren EU-Mitgliedstaaten an die europäische ETSI bezüglich Nachschlüssel?

   a) Wenn ja, welche?

   b) Wenn nein, warum nicht?

Die Fragen 4 bis 4b werden gemeinsam beantwortet.

Der Bundesregierung liegen keine Kenntnisse vor.

Die Spezifizierung von ETS (ehemals eTLS) wurde, wie in der Standardisierung üblich, von der Wirtschaft vorangetrieben. Vertreter britischer Behörden haben sich beteiligt. Andere Mitgliedsstaaten haben sich im Standardisierungsgremium nicht positioniert.

5. Wäre für die Bundesregierung eine Verschlüsselungstechnologie mit eingebauter Nachschlüssel- bzw. Abhörtechnologie vor dem Hintergrund, dass die Regierungsparteien im Koalitionsvertrag zwischen CDU, CSU und SPD festgelegt haben, dass sie „die Verbreitung sicherer Produkte und das Entwicklungsprinzip „Security by Design“ fördern“ (Zeilen: 1986 bis 1987) wollen, mit einem solchen „Security by Design“-Prinzip vereinbar?

Es wird auf die Antwort zu Frage 2 verwiesen.

6. Wird das Gütesiegel für IT-Sicherheit, wie im Koalitionsvertrag zwischen CDU, CSU und SPD vereinbart (Zeilen 1988 – 1990: „Die Einhaltung dieser über die gesetzlichen Mindeststandards hinausgehenden IT-Sicherheitsstandards werden wir Verbraucherinnen und Verbrauchern mit einem Gütesiegel für IT-Sicherheit transparent machen“), die Verschlüsselung mit Nachschlüsseln oder ähnliche Abhörmechanismen akzeptieren?

Es wird auf die Antwort zu Frage 2 verwiesen.

7. Welche Vor- und welche Nachteile sieht die Bundesregierung in Verschlüsselungstechnologien, bei denen Nachschlüssel oder ähnliche Entschlüsselungs- bzw. Eingriffstechnologien möglich sind (bitte die Vor- und Nachteile gegenüberstellen), und überwiegen für die Bundesregierung die Vor- oder die Nachteile?

Ein schwerwiegender Nachteil ist der nicht abschätzbare Schaden im Falle eines unautorisierten Einsatzes der Nachschlüssel. Zur sicheren Speicherung von Nachschlüsseln ist deshalb eine umfangreiche und hochsichere Infrastruktur notwendig, die ihrerseits aufgrund der Brisanz der gespeicherten Daten einem sehr hohen Angriffsrisiko ausgesetzt ist. Darüber hinaus wäre eine solche Infrastruktur mit einem hohen Verwaltungsaufwand und enormen Kosten verbunden.

Vorteile im Sinne der Anfrage sind keine ersichtlich.

Zudem wird auf die Antwort zu Frage 2 verwiesen.

8. Wird sich die Bundesregierung über den IT-Planungsrat und das Bundesministerium des Innern, für Bau und Heimat für den Einsatz von TLS 1.3 mit Perfect Forwarding Secrecy (PFS) in Bundesbehörden einsetzen, und welcher Zeitrahmen ist gegebenenfalls für die Implementierung angedacht?

Der „Umsetzungsplan Bund 2017“ (s. u.) sieht vor, dass die Bundesbehörden Mindeststandards, welche vom BSI auf Basis § 8 Absatz 1 BSIG veröffentlicht werden, beachten müssen. Für den Bereich der TLS-Verschlüsselung von Verbindungen existiert der „Mindeststandard des BSI zur Verwendung von Transport Layer Security (TLS)“ in Version 2.0 vom 05. April 2019. Darin wird für die Bundesverwaltung der ausschließliche Einsatz von TLS 1.2 mit Perfect Forwarding Secrecy sowie TLS 1.3 mit Perfect Forwarding Secrecy als erlaubte Verfahren festgelegt.

Darüber hinaus besteht mit der „Technischen Richtlinie TR-02102-2 (Kryptographische Verfahren: Empfehlungen und Schlüssellängen – Teil 2 – Verwendung von Transport Layer Security (TLS))“ (s. u.) eine allgemeine Empfehlung für die sichere Verwendung von TLS-Versionen sowie Cipher-Suiten. Dabei werden sowohl Cipher-Suiten mit Perfect Forward Secrecy (PFS) als auch ohne PFS empfohlen, wobei Cipher-Suiten mit PFS grundsätzlich bevorzugt werden sollen.

In dieser technischen Richtlinie werden ausschließlich TLS 1.2 sowie TLS 1.3 als sichere Verfahren für die Transportverschlüsselung genannt. Trotz der Verbesserungen, die TLS 1.3 mit sich bringt, ist TLS 1.2 bei geeigneter Konfiguration derzeit immer noch als sicher zu erachten. Daher gibt es gegenwärtig keine Pläne, die Empfehlung von TLS 1.2 in der „Technischen Richtlinie TR-02102-2“ auslaufen zu lassen.

Der Mindeststandard des BSI zur Verwendung von TLS (Version 2.0) macht TLS 1.2 mit PFS oder TLS 1.3 mit PFS für die Bundesverwaltung verpflichtend. Für Neubeschaffungen wird im Mindeststandard empfohlen, auf Kompatibilität mit TLS 1.3 zu achten. Die Dokumente sind hier online einsehbar: www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/itdigitalpolitik/up-bund-2017.pdf; www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf.

9. Auf welche Erkenntnisse kann die Bundesregierung in Bezug auf die Migration von TLS 1.0 zu TLS 1.2 hinsichtlich

   a) der finanziellen Migrationskosten (bitte nach Bundesministerien und Kostenkategorie aufschlüsseln) und

Der Bundesregierung liegen keine Informationen bezüglich finanzieller Migrationskosten vor.

   b) den zeitlichen und organisatorischen Migrationsablauf zurückgreifen (www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/BSI_veroeffentlicht_Mindeststandard_fuer_verschluesselte_Internetverbindungen_08102013.html)?

Eine vollständige Migration ist Stand heute noch nicht abgeschlossen. Einige Webseiten setzen weiterhin auf Server-Konfigurationen, welche den Einsatz von TLS 1.2 entweder nicht anbieten oder nicht ausschließlich erzwingen.

10. Sieht die Bundesregierung die im Koalitionsvertrag zwischen CDU, CSU und SPD vereinbarte Novellierung des Produktsicherheitsrechts (Zeilen 6371 – 6375: „Wir werden das Produktsicherheitsrecht novellieren, um die IT-Sicherheit in verbrauchernahen Produkten zu erhöhen. Dazu werden wir u. a. das Produkthaftungsrecht anpassen, Mindeststandards vorschreiben und die Einführung einer gewährleistungsähnlichen Herstellerhaftung prüfen.“) auch im Falle unzureichender Verschlüsselungsstandards bzw. Nachschlüssel beim Produkthersteller als ausreichend an, und wenn ja, aus welchen Gründen?

11. Bis wann beabsichtigt die Bundesregierung die im Koalitionsvertrag zwischen CDU, CSU und SPD vereinbarte Novellierung des Produktsicherheitsrechts umzusetzen?

Die Fragen 10 und 11 werden zusammen beantwortet.

Zunächst ist darauf hinzuweisen, dass schon das bestehende Recht der Produktsicherheit heute Möglichkeiten bietet, bei einer Gefahr für Sicherheit und Gesundheit von Personen aufgrund unsicherer Produkte Maßnahmen zu ergreifen.

Die Bundesregierung überprüft derzeit, ob die Regelungen des Produktsicherheitsrechts ausreichen, das bestehende Sicherheitsniveau auch im Falle von Cyberangriffen zu erhalten. Da es sich im Produktsicherheitsrecht ganz überwiegend um vollständig harmonisiertes Binnenmarktrecht handelt, werden erforderliche Nachbesserungen auf europäischer Ebene in die entsprechenden Produktsicherheitsgremien eingebracht.

Auch beim Produkthaftungsrecht handelt es sich ganz überwiegend um vollständig harmonisiertes Binnenmarktrecht. Die Europäische Kommission führt derzeit Konsultationen durch, um zu überprüfen, ob die Produkthaftungsrichtlinie im Hinblick auf technologische Neuerungen Überarbeitungen bedarf. Die Bundesregierung begleitet diese Konsultationen.

Im Übrigen wird auf die Antwort zu Frage 2 verwiesen.

12. In welchem Umfang wird die Bundesregierung bei Schäden oder Datenleaks, welche auf unzureichende Verschlüsselungstechnologien oder den Missbrauch von Nachschlüsseln zurückzuführen sind, die Herstellerhaftung verschärfen?

Da es sich bei dem Produkthaftungsrecht ganz überwiegend um vollständig harmonisiertes Binnenmarktrecht handelt, begleitet die Bundesregierung die Konsultationen der Europäischen Kommission, die überprüft, ob die Produkthaftungsrichtlinie im Hinblick auf technologische Neuerungen Überarbeitungen bedarf.

13. Welche konkreten Projekte unterstützt die Bundesregierung innerhalb der neugegründeten Agentur für Cybersicherheit (ausgestattet mit einem (Forschungs-)Budget von 200 Mio. Euro; www.heuking.de/de/news-events/fachbeitraege/der-cybersecurity-act-wohin-steuert-europa-in-fragen-der-cybersicherheit.html) hinsichtlich Verschlüsselungstechnologien, und welche finanziellen und personellen Ressourcen werden dem Thema Ende-zu-Ende-Verschlüsselungstechnologien zugewiesen?

Die Agentur für Innovation in der Cybersicherheit wurde noch nicht gegründet. Konkrete Aussagen zu den Projekten sind zu diesem Zeitpunkt deswegen noch nicht möglich.



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333